29 JAN 1981

MEMORANDUM FOR: Director of Central Intelligence



STAT FROM: [redacted]
Director of Security

SUBJECT: Strengthening the DCI's Authorities in Security Matters in the Community

1. Following your recent request, presented herein is advice as to how the DCI's authorities in security matters could be appropriately strengthened in the Intelligence Community so as to preclude repetition of a Sullivan-type case and also to reduce leaks of intelligence information.

2. Background: The heart of the problem appears to be that the DCI's statutory responsibility to protect intelligence sources and methods is not supported by commensurate authority, either statutory or through executive conferral. The logical ultimate commensurate authority would be the power to exercise a review and veto of any decision to grant access to intelligence source and method information. Currently, as reflected in DCID 1/14 (attached), each cognizant Senior Intelligence Officer (SIO) has the final authority to approve access to such intelligence information even though the ultimate statutory responsibility for its protection rests with the DCI.

Apart from the above, the DCI's responsibilities are undercut by the lack of uniformity of investigative and clearance-granting criteria in the Community. For example, the polygraph is considered to be an absolutely indispensable dimension of CIA's overall program of granting security approvals for Sensitive Compartmented Information (SCI) yet the polygraph is not used in this way by other intelligence agencies except the National Security Agency and there only for its civilian employees and contractors.

There is no consistent reinvestigation program in the Intelligence Community. The DCI 1/14, a document obviously forged five years ago by Community compromise, is imprecise in this and other significant areas.

OS 1 0228

It is felt that the DCI should have ultimate veto power over any approval for access to Sensitive Compartmented Information, that body of intelligence most vulnerable to compromise and indisputably within DCI purview. It is felt that polygraph testing, at least on counterintelligence issues, should be a prerequisite investigative procedure for access to SCI. Further, the initial granting of SCI access and the periodic revalidating of such access should be based on very similar, indeed virtually standardized, investigative and adjudicative practices throughout the Intelligence Community.

In the light of past experience with these issues, it is certain that nothing short of presidential directions will bring about the desired results. It is felt that such directions should be solicited.

3. Staff Position: Specifically, these actions appear to be appropriate.

° Acquire for the DCI the authority to review/veto the granting of access approvals for Sensitive Compartmented Information (SCI)

Under the present SCI security programming, the responsibility of the DCI to protect intelligence information and sources and methods through control of access is, in effect, delegated to Senior Intelligence Officers (SIO's) of the Intelligence Community. There is no central authority to review conflicting determinations of the SIO's or to serve as the final arbiter of a conflict. As the DCI is specifically charged to protect SCI, it is logical that he assume the role of decisionmaker when the determinations of the SIO's are contradictory with respect to the granting or continued validation of access approvals. Implicit in the role is veto power over the determination of any SIO regarding access.

In the past, efforts to strengthen or indeed establish the authority of the DCI to act within the concept of strong central direction have met with spirited resistance on the part of the Community, particularly the Office of the Secretary of Defense and the individual military services. This is illustrated in the language of the several DCID's that represent a compromise based on recognition of the DCI's responsibility but also reflecting avoidance of commonality in criteria and standards. It may be anticipated that a proposal for DCI review/veto authority will encounter the same resistance.

It should also be understood that review/veto authority could be interpreted as an invasion of the prerogatives of other agencies and departments in setting standards for hiring and retention of employees. In NSA, all employees must hold both TOP SECRET clearance and SCI access approval(s). The same is true in some measure in other components of the Defense establishment. Nevertheless, the lack of DCI veto power is not consistent with the statutory responsibility to protect intelligence sources and methods.

° Require polygraph testing as a condition of SCI access

It has long been recognized within the Agency that failure on the part of other agencies and departments to utilize the polygraph as a phase of security screening for access to SCI is inconsistent with mutual acceptance of access approvals. The CIA and NSA experience with the polygraph offers overwhelming evidence that the majority of disapproval decisions are based on polygraph-developed information. Without use of the polygraph, other members of the Intelligence Community cannot be expected to surface some of the disqualifying factors that figure in CIA and NSA adjudications. This creates two problems: Certifications cannot be accepted with any real assurance they are backed by the effective security processing permitted by polygraph screening and, in the case of other Community members, they conceivably could grant access approvals to individuals whom CIA has disapproved for access. Certification and accreditation could be approached with mutual confidence if the enhanced security attendant to use of the polygraph was a universal condition of SCI access.

CIA has argued in the past for use of the polygraph in security screening for SCI access to no avail. Personal sensibilities, institutional resistance and purported concern over civil liberty and/or legal considerations have resulted in strong opposition to acceptance of the polygraph as a tool to supplement background investigations. There is no indication that this opposition will abate. Only strong support or a directive by the Executive will condition the position of the departments and agencies which have rejected the polygraph as a screening device.

In approaching the concept of use of the polygraph for access to SCI, it is understood that any implementation must be governed by resource considerations. The undertaking will be massive and can only be accomplished in stages. The standard should be set as a matter of policy and then implemented in keeping with

the realities of the existing situation, e.g., there are not enough qualified polygraph operators available to handle the job. Further, it is not realistic to require 100% across-the-board compliance; there will be exceptions such as members of Congress and possibly Presidential appointees.

° Standardize reinvestigative policies and procedures regarding Sensitive Compartmented Information in the Community

The CIA reinvestigation program calls for investigative update, supplemented by a polygraph interview, every five years. The program has surfaced a number of security abuses that required disciplinary action. The program also serves effectively as a deterrent to those who might otherwise ignore security standards. DCID 1/14 does not require periodic reinvestigation and, of course, in the negative sense reflects current rejection by most departments and agencies of the polygraph as an investigative tool. The deterrent factor is most significant in terms of a primary concern: "leaks."

In the more general sense, failure to require periodic reinvestigation as a condition of continued access to SCI is tantamount to a determination that events that occur or circumstances that develop after granting of an initial access approval are irrelevant. This is incompatible with maintaining an effective security program.

The arguments heard from other departments and agencies against reinvestigations always stress the lack of resources. The same argument is directed against the 15-year background investigation requirement that a SECOM study recently determined directly contributed to the development of derogatory information which would not have surfaced in a 5-, 7- or even a 10-year inquiry. Gearing security processing to the capability of available resources can be dangerous, in that security standards that unquestionably contribute to the protection of classified information are abandoned or not adopted.

° Support fully the development of an automated SCI access approval data base

Currently, the U. S. Government maintains 19 computerized data bases which contain listings of persons, both in Government and industry, who hold one or more SCI access approvals. These

data bases vary in content but generally reflect the name with minimal identifying biographic data, organization, date of background investigation and access approvals currently held. The CIA maintains the most complete listing, in that it serves itself and also maintains a data base of common concern for some other agencies. Even this listing is neither complete nor totally accurate because of inefficiencies inherent in the current manual method of data input. It has been widely recognized that a requirement exists to establish a Community-wide centralized computer system which would provide current management information through an interactive data base, updated and used on-line by all member agencies through terminals located in their facilities.

This recognized need has resulted in the design of the Community-wide Computer-assisted Compartmentation Control System (4C). It is being developed in association with, but distinct from, APEX and will be operated by CIA as a service of common concern. In addition to providing an accurate and timely data base on personnel holding access approvals, it will have a memory capacity which retains data on debriefed personnel and an alert mechanism on individuals who have been declared ineligible for access or have had accesses removed for cause. It is planned that, upon activation of the 4C registry, each intelligence agency would be required to query the registry prior to the issuance of any new SCI access approval, thus learning of the SCI history of the person involved.

The 4C concept is generally well-accepted within the Community and $4,259,000 was allocated in FY 1981 for acquisition and start-up costs. In Congressional review, a $3M obligation ceiling was imposed for FY 1981 which, if retained, will cause extended start-up delays. On 15 January 1981, former DCI Turner sent letters to the Honorable Jamie L. Whitten, Chairman, House Committee on Appropriations, and the Honorable Ted Stevens, Chairman, Senate Subcommittee of Defense Appropriations, requesting restoration of funding to permit 4C installation to continue in FY 1981. Continued support for this funding restoration is vital.

5. The thoughts presented above represent the first cut at addressing the broad problem of security weaknesses in the Intelligence Community. The presentation has been framed in terms short of formal recommendations for action. This is to allow proper coordination with the offices of the General Counsel and the Legislative Counsel, a process currently underway.

STAT

Attachment

SUBJECT: Strengthening the DCI's Authorities in Security Matters in the Community

Distribution:
Orig - DCI
1 - DDCI w/o att
1 - ER w/o att
1 - A/DDA w/o att
1 - GC w/o att
1 - LC w/o att